UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

S.H., minor, by and through their legal guardian Lisa Hegge; S.C., young adult, by and through their legal guardian, Casey Curtis; E.N., minor, by and through their legal guardian Kayla Nulf; M.B.H., by and through their legal guardian Sarah Blosser, Individuals and on behalf of all others similarly situated,

Plaintiffs,

v.

POWERSCHOOL HOLDINGS, INC. and POWERSCHOOL LLC,

Defendants.

Case No.

Class Action

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff S.H., a minor, by and through their legal guardian, Lisa Hegge, Plaintiff S.C., a young adult, by and through their legal guardian, Casey Curtis, Plaintiff E.N., a minor, by and through their legal guardian Kayla Nulf, and Plaintiff M.B.H., by and through their legal guardian Sarah Blosser collectively ("Plaintiffs") bring this Class Action Complaint on behalf of themselves, and all others similarly situated ("Class Members") against Defendant PowerSchool Holdings, Inc. ("PowerSchool" or "Defendant"), through their undersigned attorneys. Plaintiffs allege, based on personal knowledge, information, and the investigation of their counsel, and facts that are a matter of public record, and upon information and belief as to all other matters as follows:

NATURE OF THE ACTION

1. This class action arises out of a December 2024 data breach (the "Data Breach") involving PowerSchool who collected and stored personally identifiable information ("PII") of Plaintiffs

2. According to PowerSchool's public notice, the "unauthorized exfiltration of personal information" compromised as a result of the Data Breach

includes names, Social Security numbers, demographic information, dates of birth, contact information, and/or medical contact information. **Exhibit A.**[1]

3. Social Security numbers specifically are known to be particularly valuable to criminals as this information can be sold and traded on the dark web black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

4. PowerSchool failed in this obligation in December 2024 (and possibly as early as August 2024) when it allowed a critical system vulnerability to be exploited thereby resulting in the Data Breach.

5. Plaintiffs and Class Members entrusted PowerSchool with all their highly sensitive PII and reasonably expected that PowerSchool would protect this information consistent with its representations.

6. Given this knowledge, PowerSchool knew or should have known that reasonable security measures were necessary to prevent unauthorized access to Plaintiffs' and Class Members' PII.

---

[1] Available at: https://www.powerschool.com/security/sis-incident/

7. The Data Breach was a direct result of PowerSchool's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII.

8. Plaintiff brings this class action lawsuit individually as well as on behalf of all those similarly situated to address PowerSchool's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party.

INTRODUCTION

9. Defendant PowerSchool is a leading provider of cloud-based education software for school administrators. Headquartered in Folsom, California, PowerSchool serves approximately 18,000 customers worldwide, including schools and school districts covering kindergarten through twelfth grade.[2]

10. As part of its educational software services, PowerSchool collects, manages, and is responsible for safeguarding the personally identifiable information

---

[2] *PowerSchool Says Hackers Stole Students' Sensitive Data, Including Social Security Numbers, in Data Breach,* TechCrunch (Jan. 9, 2025 8:16AM), PowerSchool says hackers stole students' sensitive data, including Social Security numbers, in data breach | TechCrunch.

("PII") of at least 50 million students in the United States, as well as the PII of teachers, staff, and family members.

11. According to its website, PowerSchool offers various education technology software products that help schools manage administrative tasks, including enrollment, curriculum planning, and teacher recruitment.

12. A central component of PowerSchool's offerings is its PowerSchool Student Information System ("SIS"). PowerSchool markets this product as "one secure customizable platform providing the interoperability needed to power your school and district operations with accurate student data."[3] This system is not limited to student data; it also collects information from families and staff."[4]

13. PowerSchool has repeatedly acknowledged the sensitive nature of the PII it collects and maintains. This information includes names, email addresses, phone numbers, Social Security numbers, medical details (such as food allergies and learning disabilities), dates of birth, financial information (such as reduced meal status), demographic data, and student and staff identification numbers.

---

[3] *PowerSchool SIS at-a-glance*, PowerSchool, https://https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/ (last visited March 18, 2025).

[4] *Id.*

14. As a condition of receiving education services, Plaintiffs and Class Members—students and their families—were required to provide highly sensitive PII covering nearly every aspect of their personal lives.

15. Given the sensitivity of this data and PowerSchool's public representations regarding security, PowerSchool had an obligation to protect the PII of its users, including students, teachers, and their families. However, PowerSchool failed to fulfill that obligation.

16. On or about December 19, 2024, PowerSchool's SIS system was breached due to a vulnerability (the "Data Breach"). Unauthorized parties accessed PowerSchool's systems and data by exploiting compromised credentials. Evidence suggests these parties may have gained access even earlier than December 19, 2024.

17. PowerSchool did not detect the unauthorized access or the system vulnerability until December 28, 2024.

18. PowerSchool engaged "CrowdStrike" shortly after the breach to provide an Investigation Report into this matter. (**Exhibit B)**.[5] On February 28, 2025, the CrowdStrike report was published with details about the breach and the report

[5] Available at: https://www.powerschool.com/wp-content/uploads/2025/03/PowerSchool-CrowdStrike-Final-Report.pdf.

further states there is "earlier evidence of unauthorized activity in the PowerSchool environment" occurring around August 16, 2024.

19. Public reports indicate that PowerSchool failed to implement, or improperly configured, multi-factor authentication ("MFA")—a widely recognized security practice—meant to prevent unauthorized access. Proper MFA protocols could have flagged or blocked third-party access through compromised credentials.

20. Despite its obligation, PowerSchool failed to adequately safeguard the sensitive information it collects and maintains. Recently, Senators Jim Banks (R-Ind.), Maggie Hassan (D-N.H.), and James Lankford (R-Okla.) issued a bipartisan letter calling for accountability and transparency from PowerSchool and its majority owner, Bain Capital. The Senators specifically identified critical cybersecurity failures, including the lack of multi-factor authentication, as contributing to the breach. They also condemned PowerSchool's delayed detection and notification timeline. As the Senators expressed, "significant concern about the risks that students, staff, and school districts face after malicious actors stole their personal data in a cyberattack on your company's information systems." According to the

Senators, PowerSchool's failures placed millions at risk of identity theft and underscored a serious breach of public trust. (**Exhibit C**).[6]

21. Due to PowerSchool's failure to implement effective security measures, hackers accessed and extracted vast amounts of PII belonging to students, teachers, and their families. The stolen data was exported into a .CSV file.

22. According to news reports, the hackers later threatened to release the stolen data unless PowerSchool paid a ransom. PowerSchool is suspected to have made this payment, but there is no evidence that the hackers deleted the stolen data. PowerSchool has not confirmed whether it took any steps to ensure the data was destroyed.

23. As a result of PowerSchool's negligent data retention practices, unauthorized parties accessed, viewed, downloaded, and stole highly sensitive PII from schools across the United States. Some of the stolen data dates back to 2005.

24. PowerSchool failed to provide timely notice of the Data Breach to Plaintiffs and Class Members. It did not notify affected schools until at least January 7, 2025, and in most cases, not until January 9, 2025—nearly two weeks after discovering the breach.

---

[6] Available at: https://www.banks.senate.gov/press-releases/senators-banks-hassan-and-lankford-call-for-accountability-transparency-from-powerschool-after-data-breach/.

25. In addition to being untimely, PowerSchool's notice was also insufficient. It failed to disclose critical details, including which unauthorized parties accessed the systems, how long the breach lasted, what specific data was compromised, the terms of the suspected ransom payment, and whether the stolen data has been or will be deleted.

26. Due to PowerSchool's inadequate cybersecurity measures and delayed breach notification, Plaintiffs and Class Members face an imminent risk of identity theft and fraud. Many may already be victims but cannot take protective measures because PowerSchool has not provided sufficient notice.

27. Plaintiffs and Class Members must now take steps to mitigate the risk of fraud and identity theft, including (i) placing credit freezes, (ii) setting alerts with credit reporting agencies, (iii) notifying financial institutions, (iv) closing or modifying bank accounts, and (v) monitoring credit reports for suspicious activity.

28. Plaintiffs and Class Members remain at risk because PowerSchool has not disclosed what, if any, corrective measures it has taken to secure its systems and prevent further breaches. Despite this ongoing risk, PowerSchool retains control over some of Plaintiffs' and Class Members' most sensitive PII, leaving them without assurance that their data is now secure. Plaintiffs and Class Members will not receive such confirmation until PowerSchool completes its investigation.

PARTIES

29. Plaintiff S.H. is a minor individual and citizen of the State of Michigan. Plaintiff S.H. is a student at Homer Community High School, which relied on Defendant PowerSchool to manage the PII of its students and teachers.

30. Plaintiff S.C. is a young adult individual and citizen of the State of Michigan. Plaintiff S.C. is a student at Gogebic Community College, which relied on Defendant PowerSchool to manage the PII of its students and teachers.

31. Plaintiff E.N. is a minor individual and citizen of the State of Michigan. Plaintiff E.N. is a student at Constantine High School, which relied on Defendant PowerSchool to manage the PII of its students and teachers

32. Plaintiff S.H. is a minor individual and citizen of the State of Michigan. Plaintiff S.H. is a student at Homer Community High School, which relied on Defendant PowerSchool to manage the PII of its students and teachers.

33. Plaintiff M.B.H. is a minor individual and citizen of the State of Michigan. Plaintiff S.H. is a student at Sturgis Middle School, which relied on Defendant PowerSchool to manage the PII of its students and teachers.

34. Between February and March 2024, Plaintiffs were sent a notification letter informing them of the Data Breach and that their PII may have been accessed without authorization, exfiltrated, and/or stolen. An example of such a notification letter is attached hereto as **Exhibit D**.

35. Plaintiffs relied on PowerSchool to adequately protect and manage the sensitive information entrusted to it. Plaintiff's suffered actual damages including, without limitation, time and expenses that will now be related to monitoring their financial accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of personal information, and other economic and non-economic harm. Plaintiffs and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

36. Defendant PowerSchool is a Delaware corporation founded in 1997, with its headquarters at 150 Parkshore Drive, Folsom, CA 95630. PowerSchool provides education technology products and services for schools located within Michigan and nationwide. These products and services include a Student Information System platform, document management system, enrollment and attendance manager, recruitment platform, parent communication platform, and Naviance, a tool for academic planning. In 2024, PowerSchool was acquired by Bain Capital.

JURISDICTION AND VENUE

37. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action in which the amount in controversy exceeds $5 million,

exclusive of interest and costs. The proposed class includes more than 100 members, and at least one member is a citizen of a state different from Defendant, satisfying the minimal diversity requirement. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

38. This Court has personal jurisdiction over Defendant PowerSchool because it conducts substantial business in this District, and the events giving rise to this action arise out of that business. Specifically, PowerSchool generates significant revenue from contracts with schools and school districts across all fifty states. Through these contracts, PowerSchool collects, stores, and maintains personally identifiable information (PII) and data for millions of students and teachers nationwide, including individuals within this District.

39. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claim upon which this compliant is based occurred in, were directed to, and/or emanated from this District.

FACTUAL ALLEGATIONS

A. DEFENDANT ROUTINELY COLLECTS HIGHLY SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (PII) FROM MILLIONS OF STUDENTS, TEACHERS, AND THEIR FAMILIES

40. PowerSchool is a provider of cloud-based education software for K–12 institutions across the United States. With more than 18,000 customers across North America, PowerSchool is responsible for storing and managing the PII of over fifty

(50) million students, teachers, and their family members. It retains historical data for former users of its systems dating back to 2005.[7]

41. PowerSchool serves both schools and school districts across North America. PowerSchool provides education software products allowing schools to manage administrative functions such as enrollment, attendance, parent communications, emergency contacts, grades, transcripts, assignments, medical records, and staff recruitment.

42. One software product is the "PowerSchool SIS," a database system used by at least 15,000 schools and districts nationwide.[8] A copy of the 2019 PowerSchool SIS training manual is included as **Exhibit E.**[9]

43. Upon information and belief, PowerSchool SIS is designed to allow schools and districts the ability to: collect and manage detailed information about students and staff; create student and parent portals; facilitate school

---

[7] *Hacker accessed PowerSchool's network months before massive December breach*, https://techcrunch.com/2025/03/10/hacker-accessed-powerschools-network-months-before-massive-december-breach/.

[8] *40,000 Students Start School on Time Because of 90-Day PowerSchool SIS Implementation*, PowerSchool, https://www.powerschool.com/case-studies/40000-students-start-school-on-time-because-of-90-day-powerschool-sis-implementation/ (last visited March 18, 2025).

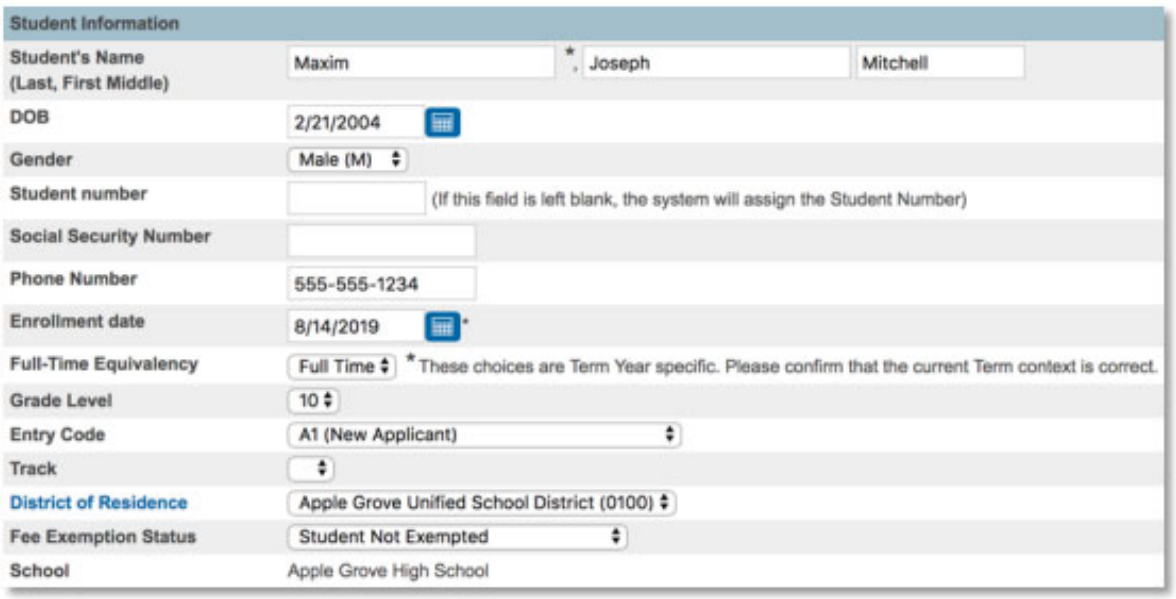
[9] Available at: https://cdnsm5-ss11.sharpschool.com/UserFiles/Servers/Server_153000/File/District/PowerSchool/PowerSchool%20SIS%20IPT%20WORKBOOK.pdf

communications; manage grades and assignments; track attendance; store health information; build schedules; and/or plan course lessons.

44. Upon information and belief, PowerSchool provides school customers training, customer support, and cybersecurity assistance upon implementing the system.

45. Students, teachers, staff, and their families within districts using PowerSchool SIS are required, as a condition of attending or working at schools, to submit data into PowerSchool's systems to receive educational services or maintain employment.

46. The PowerSchool SIS system collects and retains a broad range of highly sensitive PII, including a students' name, birth date, gender, social security number, phone number, and enrollment date.



Student Information				
Student's Name (Last, First Middle)	Maxim	* Joseph	Mitchell	
DOB	2/21/2004			
Gender	Male (M)			
Student number		(If this field is left blank, the system will assign the Student Number)		
Social Security Number				
Phone Number	555-555-1234			
Enrollment date	8/14/2019 *			
Full-Time Equivalency	Full Time * These choices are Term Year specific. Please confirm that the current Term context is correct.			
Grade Level	10			
Entry Code	A1 (New Applicant)			
Track				
District of Residence	Apple Grove Unified School District (0100)			
Fee Exemption Status	Student Not Exempted			
School	Apple Grove High School			

Exhibit E, pg. 26

47. The PowerSchool SIS system can also collect and retain other highly sensitive PII including emergency/medical contact information; device identifiers (e.g., unique device ID, IP address, cookies); health (e.g., immunization records); Academic grades; Standardized test scores; and information regarding learning disabilities. (*see* **Exhibit E**, pgs. 14-15).

48. According to its Global Privacy Statement, PowerSchool collects PII through various means, including:[10]

- Directly from users (e.g., when creating accounts)
- Automated technologies (e.g., cookies and tracking pixels)
- Third-party sources (e.g., data analytics providers)

49. The PII collected by PowerSchool is highly sensitive and, if accessed by unauthorized parties, can be exploited for identity theft, financial fraud, and other forms of harm.

50. This information is also protected by federal law, including the Family Educational Rights and Privacy Act (FERPA), which prohibits the unauthorized disclosure of student records.

51. As the custodian of such data, PowerSchool had a duty to implement reasonable safeguards to protect the PII it collects—particularly confidential student

[10] *https://www.powerschool.com/privacy/*

records belonging to Plaintiffs and Class Members—from unauthorized access or disclosure.

52. PowerSchool was further obligated to honor the representations it made to the public regarding the security and protection of PII.

B. DEFENDANT TOUTED ITS DATA SECURITY SAFEGUARDS

53. PowerSchool knew, or was negligent in not knowing, that it had a duty to protect its customers' and users' highly sensitive personally identifiable information (PII) and student records from unauthorized disclosure.

54. PowerSchool's legal duty to safeguard this data arises from the Family Educational Rights and Privacy Act (FERPA), other applicable federal and state laws, common law principles, industry standards, and its own public statements regarding cybersecurity and privacy.

55. Independent of its legal obligations, PowerSchool made explicit and repeated public assurances that it could be trusted to protect the sensitive PII and educational records it collects.

56. PowerSchool acknowledged its responsibility to protect data on its own website, stating: "the safe collection and management of student data is essential to

student success in the digital classroom."[11] It further emphasized that it "knows the importance of understanding state-specific regulations, solving students' and educators' unique challenges, and supporting the needs of the local community."[12]

57. PowerSchool made numerous representations to customers, users, and the public about the security of its data systems, including the following:

- "PowerSchool has signed the national Student Privacy Pledge regarding the collection, maintenance, and use of student personal information. The pledge states: 'School service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security.'"[13]
- "PowerSchool certifies the application database, and infrastructure security of our software solutions."[14]
- "PowerSchool employs a variety of physical, administrative, and

---

[11] *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited March 18, 2025).

[12] *Personal Education for Every Journey*, PowerSchool, https://www.powerschool.com/ (last visited March 18, 2025).

[13] *Student Data Privacy: Everything you Need to Know*, PowerSchool, https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ (last visited March 18, 2025).

[14] *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited March 18, 2025).

technological safeguards designed to protect your data against loss, misuse, and unauthorized access or disclosure. ***We strive to continuously maintain reasonable physical, administrative, and technical security measures.*** Our security measures consider the type and sensitivity of the data being collected, used, and stored, and the current state of technology and threats to data. Defendant independently verifies its security management system to the internationally recognized standard for security management and holds ISO 27001 and SOC2 certifications. Defendant also endeavors to align its privacy and security operations to best practices and relevant international regulations."[15]

- "PowerSchool is committed to being a good custodian of student data – taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability. The company believes that the safe collection and management of student data is essential to

[15] *Privacy,* PowerSchool (last updated Feb. 2, 2023) https://www.powerschool.com/legal/privacy-2023/.

student success within the 21st Century digital classroom."[16]

- "[T]he PowerSchool Information Security Report was born out of the K- 12 Education Technology Secure by Design Pledge . . . The report is meant to provide our customers with additional transparency about cybersecurity at PowerSchool."[17]
- "We are dedicated to protecting your students' data with a comprehensive security program that starts with 'secure by design' principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center. Our products are independently validated by third-party auditors, ensuring your data is always protected with PowerSchool."[18]
- "PowerSchool's commitment to being the most trusted edtech leader in student privacy protection and cybersecurity extends to our AI

---

[16] *Student Data Privacy: Everything you Need to Know*, PowerSchool (June 20, 2023) https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/.

[17] *Cybersecurity, Data Privacy, & Infrastructure,* PowerSchool, https://www.powerschool.com/security/ (last visited March 18, 2025).

[18] *PowerSchool SIS*, PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last visited March 18, 2025).

applications. We ensure that security best practices are incorporated during research and development as well as protecting our applications and customer data."[19]

- "We're dedicated to best-in-class security in our interoperable products, as a company, and with our employees . . . we have the right security professionals, we have scale, and we want to take the discipline of data security even further."[20]

58. PowerSchool further claimed compliance with FERPA, the General Data Protection Regulation (GDPR), the Children's Online Privacy Protection Act (COPPA), "Breach Laws," and other applicable laws, offering additional assurances that users' data would be properly safeguarded.[21]

59. Through these statements, PowerSchool misrepresented the actual security of its systems and the safety of the sensitive PII and educational records it collected. PowerSchool was negligent or reckless in making these claims despite

---

[19] *Responsible AI with Security by Design*, PowerSchool (Nov. 28, 2023) https://www.powerschool.com/blog/bring- ai-to-data/.

[20] *5 Ways Tech Directors Can Improve Student Data Security and Privacy Through Interoperability*, PowerSchool (Aug. 26, 2022) https://www.powerschool.com/blog/ways-tech-directors-can-improve-student-data-security-privacy-through-interoperability/.

[21] *See Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited March 18, 2025).

operating platforms with significant cybersecurity vulnerabilities, as further discussed below.

60. Even after suffering a large-scale data breach in December 2024, PowerSchool continued to misrepresent the security of its products. As of January 17, 2025, PowerSchool's website still claimed it is a "good custodian of student data, taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability."[22] Several examples of PowerSchool's current public-facing representations regarding the security of its products are reproduced below:

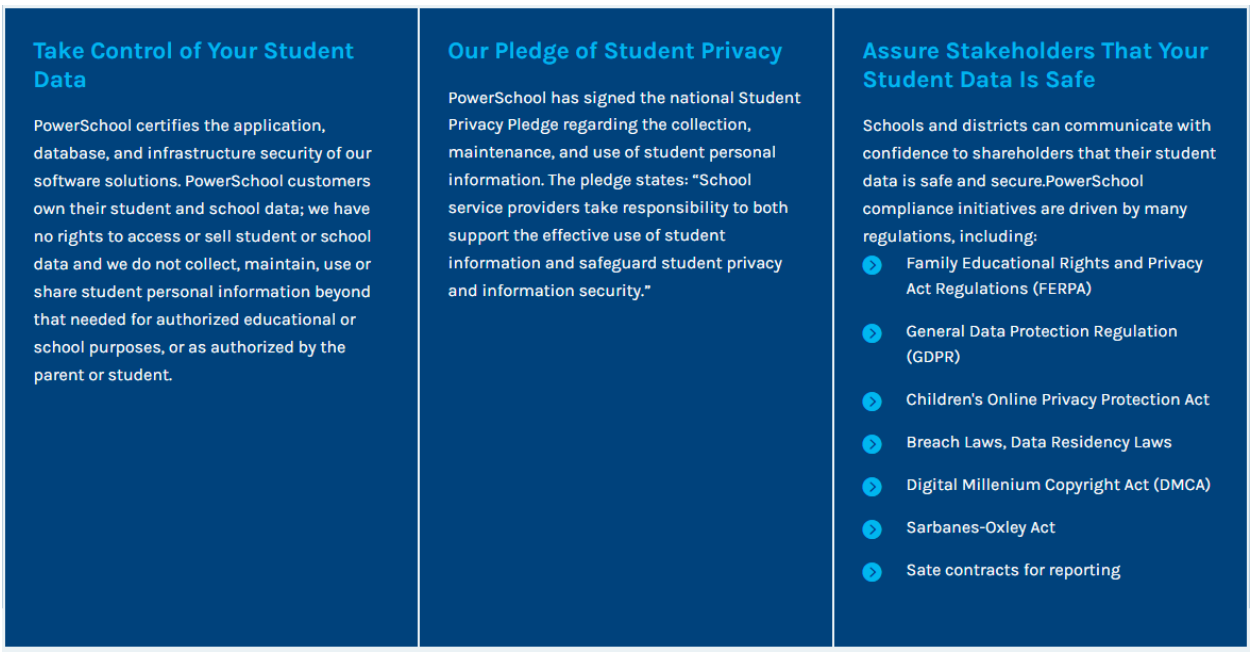
- "PowerSchool certifies its software solutions' application, database, and infrastructure security."[23]
- "Parents can rest assured that PowerSchool is a trusted, verified custodian of their children's data."[24]

---

[22] *Id.*

[23] *Student Data Privacy: Everything You Need to Know,* PowerSchool (June 20, 2023), https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/.

[24] *Cybersecurity, Data Privacy, & Infrastructure*, PowerSchool, https://www.powerschool.com/security/ (last visited March 18, 2025).



Take Control of Your Student Data

PowerSchool certifies the application, database, and infrastructure security of our software solutions. PowerSchool customers own their student and school data; we have no rights to access or sell student or school data and we do not collect, maintain, use or share student personal information beyond that needed for authorized educational or school purposes, or as authorized by the parent or student.

Our Pledge of Student Privacy

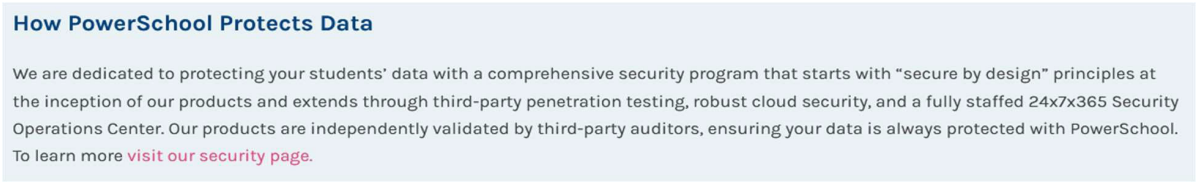
PowerSchool has signed the national Student Privacy Pledge regarding the collection, maintenance, and use of student personal information. The pledge states: "School service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security."

Assure Stakeholders That Your Student Data Is Safe

Schools and districts can communicate with confidence to shareholders that their student data is safe and secure.PowerSchool compliance initiatives are driven by many regulations, including:

- Family Educational Rights and Privacy Act Regulations (FERPA)
- General Data Protection Regulation (GDPR)
- Children's Online Privacy Protection Act
- Breach Laws, Data Residency Laws
- Digital Millenium Copyright Act (DMCA)
- Sarbanes-Oxley Act
- Sate contracts for reporting

- "We are dedicated to protecting your students' data with a comprehensive security program that states with 'secure by design' principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center. Our products are independently validated by third-party auditors, ensuring your data is always protected with PowerSchool."[25]



How PowerSchool Protects Data

We are dedicated to protecting your students' data with a comprehensive security program that starts with "secure by design" principles at the inception of our products and extends through third-party penetration testing, robust cloud security, and a fully staffed 24x7x365 Security Operations Center. Our products are independently validated by third-party auditors, ensuring your data is always protected with PowerSchool. To learn more visit our security page.

[25] *PowerSchool SIS,* PowerSchool, https://www.powerschool.com/student-information-cloud/powerschool-sis/ (last visited March 18, 2025).

61. Based on these representations, Plaintiffs and Class Members entrusted PowerSchool with their highly sensitive PII and educational records as a condition of receiving education or employment services, relying in part on PowerSchool's assurances about its data security systems.

C. CONTRARY TO DEFENDANT'S ASSURANCES, POWERSCHOOL FAILED TO ADEQUATELY SAFEGUARD USER PII

62. Despite PowerSchool's representations, it has failed to issue direct notice of the Data Breach to all individuals whose personal information was compromised—including students, teachers, staff, and their families.

63. To date, PowerSchool has limited its correspondence regarding the Data Breach to a generic customer letter sent only to institutional clients, which included minimal details about affected individuals. A copy of this letter is attached as **Exhibit F**.

64. On or about January 13, 2024, PowerSchool sent a *Notice of Data Breach* (the "Notice") to its school customers. (**Exhibit G**).[26] The Notice stated, in relevant part:

> On December 28, 2024, we became aware of a potential cybersecurity incident involving unauthorized access to certain PowerSchool Student Information System (SIS) information through one of our community-focused customer portals, PowerSource.

---

[26] An archived copy available at: https://tinyurl.com/WebArchive-PowerSchool-Notice

* * *

> On January 7, 2025, we proactively communicated this incident to the PowerSchool SIS customers affected by this incident, and we continue to support them through next steps. Districts and schools that do not utilize PowerSchool SIS were not affected. If you are a parent or guardian who wants to know if your school was involved, please reach out to your school directly.
>
> * * *
>
> Across our customer base, we have determined that for a portion of individuals, some personally identifiable information (PII), such as social security numbers (SSN) and medical information, was involved. We are working with urgency to complete our investigation and identify the individuals whose data may have been involved.

65. Although PowerSchool claims to have discovered the breach on December 28, 2024, it appears it did not issue any form of public or individual notice until at least January 7, 2025, by which time unauthorized actors had already accessed, viewed, and exfiltrated the personal and educational data of Plaintiffs and Class Members.

66. On information and belief, PowerSchool reported the Data Breach to the California Attorney General's office on January 27th, 2024.[27] PowerSchool's also informed the California Attorney General the breach occurred during the dates of December 19, 2024, through December 28, 2024.

---

[27] *See*, https://tinyurl.com/California-Attorney-General

67. PowerSchool's March 7, 2025, public "Cybersecurity Incident" notice states that by "January 27, 2025, PowerSchool began the process of filing regulatory notifications with Attorneys General Offices across applicable U.S. jurisdictions on behalf of impacted customers who have not opted-out of our offer to do so."[28]

68. As of this filing, PowerSchool has offered no explanation for the significant delay in providing public notification regarding the Data Breach or the delay in providing personal notification to the Plaintiffs and Class Members regarding the Data Breach. PowerSchool has therefore failed to provide sufficient or timely notice of the breach to affected individuals.

69. PowerSchool's delay likely violates the Michigan Identity Theft Protection Act, Mich. Comp. Laws § 445.72, and renders its prior security and privacy assurances misleading in violation of the Michigan Consumer Protection Act, Mich. Comp. Laws § 445.903.

70. Instead, before January 27th, PowerSchool had instructed individuals to "reach out to your school directly" to determine whether their or their children's data was compromised.[29]

---

[28] PowerSchool's March 7, 2025 "*SIS Incident*" notice available at: https://www.powerschool.com/security/sis-incident/

[29] PowerSchool's January 13, 2025 "*SIS Incident*" notice available at: https://tinyurl.com/WebArchive-PowerSchool-Notice

71. On or about January 30th, PowerSchool provided a webpage indicating steps individuals within the United States could take if they were notified about the breach.[30]

72. On information and belief, PowerSchool has not publicly disclosed the full scope of the breach, nor identified which users or types of data were affected.

73. On information and belief, PowerSchool has not confirmed how many of the approximately fifty (50) million student records it stores were impacted, nor has it indicated when—if ever—it will provide comprehensive notice to the affected parties.

74. The size and scope of the breach are extensive. News outlets have described the incident as "close to being the worst-case scenario cyber incident for the K-12 sector."[31]

---

[30] PowerSchool's "*Notice of Data Breach For Individuals in the United States*" available at: https://tinyurl.com/PowerSchool-US-Notice

[31] Loraine Langreo, *Close to a 'Worst-Case Scenario': Cybersecurity Expert Discusses PowerSchool's Data Breach*, EDUCATION WEEK (Jan. 14, 2025), https://www.edweek.org/technology/close-to-a-worst-case-scenario- cybersecurity-expert-discusses-powerschools-data-breach/2025/01.

75. One report claims the "hacker who breached" the PowerSchool system "claimed in an extortion demand that they stole the personal data of 62.4 million students and 9.5 million teachers."[32]

76. Independent investigations suggest that the breach also affected former PowerSchool customers, with some districts reporting compromised student numbers four to ten times higher than their current enrollment.[33]

77. The breach's impact is likely to grow as PowerSchool's investigation continues and more affected data and individuals are identified.

78. Because the investigation remains ongoing, Plaintiffs and Class Members have no way to assess the full extent of the breach or how their sensitive information may be misused.

79. According to the Notice, the breach occurred through the use of a compromised credential—i.e., valid login information accessed by an unauthorized party.

---

[32] https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/.

[33] PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data, *TechCrunch* (Jan. 15, 2025 9:45AM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/.

80. A February 28, 2025, CrowdStrike report confirms the breach occurred through the use of compromised credentials, and the report further confirms that "earlier evidence of unauthorized activity in the PowerSchool environment associated with the compromised support credentials between August 16, 2024 and September 17, 2024." **(Exhibit B.)**

81. On information and belief, such compromises often occur when users reuse passwords, fail to update them regularly, or choose weak or easily guessed passwords. These insecure practices allow malicious actors to exploit stolen credentials available on the black market or to crack passwords using automated tools.

82. On information and belief, one known safeguard against compromised credentials is multi-factor authentication ("MFA"), which requires an additional verification step beyond a password.

83. According to one publication, "[h]ad 2FA been active, hackers would've had to pass a second checkpoint to successfully access PowerSchool's internal systems."[34] This publication even states "[h]ad 2FA been active, hackers

[34] https://www.pcworld.com/article/2611711/powerschool-simple-security-error-was-avoidable-you-can-do-better.html

would've had to pass a second checkpoint to successfully access PowerSchool's internal systems" and that "PowerSchool made a mistake in not enforcing MFA."

84. MFA can include a randomly generated code, biometric input, or a physical device, adding a critical layer of protection for user accounts.

85. The use of MFA is widely regarded as essential by cybersecurity experts and institutions such as the National Institute of Standards and Technology (NIST) and Microsoft.[35]

86. On information and belief, PowerSchool failed to implement MFA or used an improperly configured version, despite its well-documented efficacy and industry recognition as a best practice.[36]

---

[35] *Multi-Factor Authentication*, NIST (last updated March 12, 2024) https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication; *What is: Multifactor Authentication*, Microsoft, https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437- 121c-be60-d123-eda06bddf661 (last visited March 18, 2025).

[36] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data,* TechCrunch (Jan. 15, 2025 9:45AM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all- historical-student-and-teacher-data/ .

87. Industry standards also recommend the deletion of PII once it is no longer necessary for business operations. As NIST states, "[i]f PII is no longer relevant and necessary, then PII should be properly destroyed."[37]

88. Disposing of obsolete data reduces the volume of potentially exposed information in the event of a breach.

89. On information and belief, PowerSchool retained sensitive user data—including that of former students and employees—dating back to the 2009–2010 school year.[38]

90. On information and belief, this retained data, including educational records and PII, was not encrypted, making it easier for unauthorized actors to access, use, and exploit.

91. Despite these failures, PowerSchool publicly asserts that it "take[s] responsibility to protect student, family, and educator data privacy extremely

---

[37] *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* NIST (Apr. 2010), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf .

[38] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data*, TechCrunch (Jan. 15, 2025 9:45PM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all- historical-student-and-teacher-data/.

seriously, and [is] committed to taking further steps to strengthen the security of our systems."[39]

92. Despite this notice, PowerSchool has not disclosed critical information about the cause of the breach, the vulnerabilities exploited, the identity of the unauthorized third party, or the remedial measures it has undertaken.

93. The only complete disclosure to date is the February 2025 CrowdStrike report which states "[b]etween December 19, 2024, at 23:02:54 UTC, and December 23, 2024, at 08:04:45 UTC, the Threat Actor exfiltrated data from the Teachers and Students tables of the PowerSchool SIS instances for certain PowerSchool customers[.]" (**Exhibit B**).

94. PowerSchool's notice regarding the Data Breach is deficient. Not only has PowerSchool failed to send it to affected individuals directly, but it also omits key facts necessary for Plaintiffs and Class Members to protect themselves from harm. Specifically, PowerSchool has not:

- disclosed which individuals were impacted;
- identified the party or parties responsible;
- explained which systems were compromised; or

[39] PowerSchool's March 7, 2025 "*SIS Incident*" notice available at: https://www.powerschool.com/security/sis-incident/

- stated how long the unauthorized access lasted or what data was taken.

95. Plaintiffs' and Class Members' information is at serious risk of misuse, including:

- sale on the dark web;
- use in criminal activity; or
- exploitation for unauthorized marketing.

96. The full extent of the breach remains unknown. According to just one report, the breach involved the "personal data of 62.4 million students and 9.5 million teachers."[40]

97. But these estimated numbers pertain to just the December 2024 unauthorized access. It is unknown whether information was compromised by the unauthorized access occurring between August 2024 and September 2024 because the PowerSchool "SIS log data did not go back far enough[.]" (**Exhibit B**).

98. PowerSchool continues to maintain Plaintiffs' and Class Members' data, and there is no assurance the breach has been fully contained or that adequate protections are now in place. As such, their sensitive information remains vulnerable to further exposure, misuse, and exploitation.

---

[40] https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/

D. COMPROMISED DATA IS HIGHLY VALUABLE TO HACKERS AND CYBERCRIMINALS

99. Cyberattacks by hackers and other cybercriminals are widespread and growing in frequency. According to a recent Forbes report, the number of data breaches exceeded 1,571 in the first half of 2024—a 14% increase compared to the same period in 2023.[41]

100. Educational institutions and their affiliated vendors are acutely aware that their databases are prime targets for cybercriminals, largely because they store substantial amounts of personally identifiable information (PII), including confidential student records. Data breaches affecting education-related organizations are becoming increasingly common.[42] A 2022 report published by the United States Government Accountability Office notes that:

> according to data from the MS-ISAC, reported ransomware incidents against K-12 schools increased significantly in August and September 2020. ***Fifty-seven percent of all ransomware incidents reported to the MS-ISAC involved K-12 schools***, compared to 28 percent of reported

---

[41] *There are 1 billion victims of data breaches so far this year. Are you one of them, USA Today* (July 18, 2024 5:10 a.m.), https://www.usatoday.com/story/money/2024/07/18/data-breach-what-to-do/74441060007/.

[42] *One Reason School Cyberattacks Are On the Rise? Schools Are Easy Targets for Hackers,* NPR (Mar. 11, 2024 12:00 p.m.), https://www.npr.org/2024/03/11/1236995412/cybersecurity-hackers-schools-ransomware.

ransomware incidents around the end of the 2019-2020 school year (January through July 2020).[43]

101. Hackers place a high value on education-related PII. Studies have shown that PII is more valuable to cybercriminals than other types of data, such as credit card numbers or login credentials. This is because "criminals can compile more PII from the dark web to then engage in harder to prevent fraud or full-on identity theft."[44]

102. Cybercriminals actively seek to gather PII because individual data points can "be pieced together like a puzzle" to "complete an online profile of" a person and "impersonate you or others online."[45] Beyond identity theft, hackers also traffic in PII to profit from its sale on underground marketplaces.

---

[43] *Critical Infrastructure Protection: Additional Federal Coordination is Needed to Enhance K-12 Cybersecurity,* U.S. Government Accountability Office (Oct. 20, 2022), https://www.gao.gov/assets/gao-23-105480.pdf.

[44] *Hackers Went After Personally Identifiable Information the Most, Study Says,* SC Media (Jan. 5, 2023), https://www.scworld.com/news/hackers-went-after-personally-identifiable-information-the-most-study-says.

[45] *What is PII and Why Criminals Want Yours,* Cyber Defense Magazine (Feb. 28, 2019), https://www.cyberdefensemagazine.com/what-is-pii-and-why-criminals-want-yours/.

103. Experian describes the dark web as "a huge marketplace for stolen data and personal information,"[46] where data obtained from breaches is frequently bought and sold. This report is confirmed by PreyProject which states the "Dark Web serves as a pivotal platform for cybercriminals, facilitating the sale and purchase of stolen data, including credentials, financial information, and software exploits."[47]

104. As a result, Plaintiffs and Class Members face an imminent risk that their PII—which was accessed, viewed, and downloaded in the Data Breach—will be sold on the dark web.

105. Consumer data commands significant value on the dark web. According to CyberDefense Magazine, the average price for a consumer's passwords is approximately $80, while even minor data points such as purchase history may sell for $20. Credit card numbers can be sold for as little as $5, whereas passports may command up to $2,000.[48]

---

[46] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[47] https://preyproject.com/blog/lifecycle-stolen-credentials-dark-web#:~:text=and%20financial%20fraud.-,The%20Journey%20of%20Stolen%20Credentials%20in%20the%20Dark%20Web,into%20various%20forms%20of%20cybercrime.

[48] Cyber Defense Magazine, *supra* note 40.

106. A Dark Web Price Index published by Privacy Affairs found that a comprehensive set of documents and account credentials sufficient to commit identity theft typically sells for around $1,000.[49]

107. Student records are especially attractive to identity thieves because they often contain full personal profiles. Moreover, students are more likely to have little or no credit history, making their identities particularly useful for fraudulent financial activities.

108. PowerSchool has even confirmed that "[a]ccording to the U.S. Dept. of Education, the value of a student record on the black market is $250 to $350."[50] PowerSchool therefore states "[p]rotecting their data privacy is essential for both their potential as a vulnerable target and for maintaining the integrity and safety of their education journey." *Id.*

---

[49] *Revealed – How Much is Personal Information Worth on the Dark Web?* Insurance Business (May 1, 2023) https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information- worth-on-the-dark-web-444453.aspx .

[50] *Student Data Privacy: Everything You Need to Know*, PowerSchool (Jun. 20, 2023), https://www.powerschool.com/blog/student-data-privacy-everything-you-need-to-know/ .

109. PowerSchool is fully aware of the cybersecurity risks facing educational organizations. These risks are especially apparent given PowerSchool's prior experience with data breaches and cyberattacks.[51]

E. DEFENDANT FAILED TO IMPLEMENT REASONABLE SAFEGUARDS FOR PLAINTIFFS' AND CLASS MEMBERS' PII

110. Defendant PowerSchool failed to implement reasonable data security safeguards consistent with regulatory guidance and widely accepted industry standards appropriate to the sensitive nature of the personal identifiable information (PII) at issue. As a result of PowerSchool's negligence, unauthorized third parties accessed, viewed, and downloaded Plaintiffs' and Class Members' highly sensitive PII during the Data Breach. PowerSchool disregarded numerous guidelines issued by government agencies and industry experts and failed to adopt appropriate measures.

---

[51] *Cybersecurity, Data Privacy, & Infrastructure,* PowerSchool, https://www.powerschool.com/security/ (last visited March 18, 2025).

1. Regulatory Requirements and Guidelines

111. The Federal Trade Commission ("FTC") has issued specific guidance regarding reasonable data security practices. In its publication, *Start with Security: A Guide for Business*, the FTC instructs businesses to identify the personal information they collect, retain only what is necessary, protect retained data, properly dispose of unneeded information, and develop a response plan for security incidents[52]

112. The FTC further advises businesses to take reasonable steps to secure personal data. This includes limiting access to personal information based on job necessity, establishing separate user accounts to control access to data, and ensuring that employees without a business need do not have access to sensitive information.[53]

113. The FTC also emphasizes the importance of securing sensitive personal data during both storage and transmission. It recommends the use of strong encryption and the designation of informed personnel capable of evaluating and implementing appropriate data security protocols.[54]

---

[52] Fed. Trade Comm'n, *Start with Security: A Guide for Business (*Aug. 2023*)*, https://www.ftc.gov/business- guidance/resources/start-security-guide-business .

[53] *Id.*

[54] *Id.*

2. Industry Standards

114. The National Institute of Standards and Technology ("NIST") provides widely recognized cybersecurity guidance intended to help organizations of all sizes manage and reduce cybersecurity risk. According to NIST, passwords alone are insufficient for protecting sensitive information. NIST recommends the use of multi-factor authentication (MFA) to verify user identity through more than just a username and password.[55]

115. PowerSchool failed to implement or require appropriate access controls, including MFA, and lacked adequate authorization protocols to protect its systems and networks. This failure contributed directly to the Data Breach.[56]

116. The NIST Cybersecurity Framework also advises that organizations should collect and retain personally identifiable information only when it is directly

---

[55] *Understanding the NIST Cybersecurity Framework*, Fed. Trade Comm'n, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last visited March 18, 2025).

[56] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data*, TechCrunch (Jan. 15, 2025 9:45AM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/.

relevant and necessary for a legitimate business purpose. Retention should be limited to the duration necessary to accomplish that purpose.[57]

117. Contrary to this guidance, PowerSchool retained PII long after it ceased to serve a valid business purpose—including information related to individuals who were no longer enrolled in or employed by school-customers—dating back to at least the 2009–2010 academic year.[58]

118. PowerSchool disregarded applicable FTC and NIST guidance and best practices, thereby failing to protect Plaintiffs' and Class Members' highly sensitive PII and educational records from unauthorized access and disclosure.

119. The Data Breach could have been prevented had PowerSchool implemented reasonable security and privacy measures recommended by Federal and State agencies and industry authorities. These measures included encryption of stored and transmitted PII, the use of MFA, and the timely destruction of data that was no longer necessary.

---

[57] *SA-8 (33): Minimization*, CSF Tools, https://csf.tools/reference/nist-sp-800-53/r5/sa/sa-8/sa-8-33/ (last visited March 18, 2025).

[58] *PowerSchool Data Breach Victims Say hackers Stole 'All' Historical Student and Teacher Data*, TechCrunch (Jan. 15, 2025 9:45AM), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/.

120. PowerSchool's lack of adequate safeguards is especially concerning given the numerous warnings about predictable cybersecurity and privacy threats in the education sector. Despite being fully aware of these risks, PowerSchool did not take the necessary measures to protect the data of the Plaintiffs and Class Members.

121. PowerSchool's misconduct is further exacerbated by its own public recognition of the dangers posed by cyberattacks and identity theft. For instance, PowerSchool has publicly acknowledged that "From 2018 to 2022, 2 million students have been affected by ransomware attacks, and in 2022 alone, data was exfiltrated in at least 58 school incidents. Globally, 56% of K–12 schools experienced a cyberattack." [59]

122. By making these statements, PowerSchool conveyed to the public that it comprehended the risks and was committed to cybersecurity. These assurances led Plaintiffs and Class Members to reasonably believe that their Personally Identifiable Information (PII) would be safeguarded.

---

[59] *4 Reasons Why a Robust K-12 SIS is a Smart Long-Term Investment*, PowerSchool (June 2, 2023) https://www.powerschool.com/blog/4-reasons-why-a-robust-sis-is-a-smart-long-term-investment/.

F. THE DATA BREACH WILL RESULT IN ONGOING IDENTITY THEFT AND FRAUD

123. As a direct consequence of the Data Breach—caused by Defendant's misconduct—Plaintiffs and Class Members face a heightened and imminent risk of identity theft and fraud. In many cases, Plaintiffs and Class Members may have already fallen victim to such harm without their knowledge. Moreover, breaches like the one at issue here cause significant disruption to individuals' daily lives and financial stability.

124. Plaintiffs and Class Members are now exposed to multiple forms of identity theft, including but not limited to financial identity theft, medical identity theft, criminal identity theft, synthetic identity theft, and child identity theft. These forms of identity theft can lead to serious fraudulent activity, such as unauthorized credit card use, exploitation of government benefits, bank fraud, employment-related fraud, tax return fraud, and misuse of medical records or insurance.[60]

125. The risk of identity theft after a data breach is both enduring and well-documented. A 2017 study by Javelin Strategy & Research found that fraud

---

[60] *A Guide to Identity Theft Statistics for 2025*, McAfee, https://www.mcafee.com/learn/a-guide-to-identity-theft-statistics/ (last visited March 18, 2025).

involving data that is two to six years old surged by nearly 400%, highlighting the prolonged period during which breach victims remain susceptible.[61]

126. Children are especially vulnerable to identity theft when their sensitive personal information is compromised. That is because any "fraud typically takes place years after a child's personally identifiable information (PII) [was] initially breached."[62] And the "damage caused by child identity theft can vary from a single fraudulent bill in collections to a foreclosed mortgage."[63]

127. One of the most significant reasons a children are especially vulnerable to identity theft is because "[c]reditors do not verify age of applicants data."[64] Thus, the potential misuse of the data "go undetected until a child becomes an adult and seeks credit, only to find a history of falsely obtained credit in existence."[65]

128. Any remedial measures PowerSchool may offer will be inadequate to fully protect Plaintiffs and Class Members, including the minors, from the long-term and ongoing risks of identity theft and fraud.

---

[61] Experian, *supra* note 22.

[62] https://javelinstrategy.com/sites/default/files/files/reports/21-5012J-FM-2021%20Child%20Identity%20Fraud%20Study_1.pdf

[63] https://dos.ny.gov/what-you-should-know-about-child-identity-theft.

[64] *Id*.

[65] *Id*.

129. PowerSchool has yet to provide timely notification to those affected, and any delayed measures to address the breach may be too late to prevent substantial harm.

G. PLAINTIFFS AND CLASS MEMBERS SUFFERED DAMAGES

130. The Data Breach was the direct and proximate result of PowerSchool's failure to adequately safeguard Plaintiffs' and Class Members' personal and educational information from unauthorized access, use, and disclosure.

131. PowerSchool's conduct violated FERPA, various other federal and state laws and regulations, applicable industry standards, and common law duties.

132. PowerSchool failed to implement appropriate administrative, technical, and physical safeguards necessary to ensure the security and confidentiality of the data, and to protect against reasonably foreseeable threats to its integrity and unauthorized disclosure.

133. Plaintiffs' and Class Members' personally identifiable information (PII) and educational records are highly sensitive and private. PowerSchool failed to provide adequate protections for this information.

134. PowerSchool also failed to obtain Plaintiffs' and Class Members' consent before disclosing their personal and educational data to unauthorized third parties, in violation of applicable legal and industry standards.

135. As a direct and proximate result of PowerSchool's acts and omissions—and the resulting Data Breach—Plaintiffs and Class Members now face an imminent, ongoing, and heightened risk of identity theft and fraud.

136. To mitigate these risks, Plaintiffs and Class Members have been forced to take precautionary steps that they otherwise would not have needed to undertake. These steps include but are not limited to: (i) placing credit freezes; (ii) setting up fraud alerts with credit reporting agencies; (iii) notifying financial institutions; (iv) alerting medical providers; (v) closing or modifying financial accounts; and (vi) regularly monitoring credit reports and other financial records for unauthorized activity.

137. PowerSchool's misconduct directly caused the Data Breach, which exposed highly sensitive PII and educational records without Plaintiffs' and Class Members' knowledge or consent. As a result, Plaintiffs and Class Members have suffered—and continue to suffer—economic loss and other actual harm, including: (i) the theft of valuable PII, including medical information and student records; (ii) imminent risk of identity theft; (iii) the inability to meaningfully mitigate these risks due to PowerSchool's delayed notification; (iv) the loss of privacy; and (v) out-of-pocket expenses and time spent addressing the consequences of the breach.

138. Although Plaintiffs' and Class Members' data has already been compromised, PowerSchool still retains copies of this sensitive information.

Plaintiffs and Class Members therefore have a vested and ongoing interest in ensuring that their data is secured and protected from any further unauthorized access or disclosure.

CLASS ALLEGATIONS

139. Plaintiffs bring this action on behalf of themselves, and all others similarly situated pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

140. Plaintiff proposes the following Class, subject to amendment as appropriate:

- All persons identified by PowerSchool Holdings, Inc. whose personally identifiable information ("PII") was compromised, accessed, or disclosed in the breach that is the subject of the Notice of Data Breach that Defendant PowerSchool Holdings, Inc. distributed on or about January 7, 2025.

141. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

142. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

143. **Numerosity:** The precise number of Class Members is presently unknown to Plaintiffs but is ascertainable from Defendant's records. Joinder of all Class Members is impracticable, as the Class likely consists of thousands of individuals. PowerSchool maintains data for ~60 million students, many of whom, along with their guardians, may be Class Members. Additionally, over 77 school districts across the United States have been affected. Notice can be provided through mail, email, internet postings, publications, and other means as directed by the Court.[66]

144. **Commonality:** Common questions of law and fact predominate over individualized issues. These include, but are not limited to:

1. Whether Defendant owed a duty to protect the PII of Plaintiffs and the Class;

2. Whether Defendant had a duty to prevent unauthorized disclosure of PII;

---

[66] Lawrence Abrams, *PowerSchool hack exposes student, teacher data from K-12 districts*, BLEEPING COMPUTER (Jan. 7, 2025), https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data- from-k-12-districts/ .

3. Whether Defendant failed to reasonably safeguard Plaintiffs' and the Class's PII;

4. Whether Defendant timely discovered and disclosed the breach;

5. Whether Defendant's security practices were reasonable under the circumstances;

6. Whether Defendant engaged in unfair, unlawful, or deceptive practices;

7. Whether Plaintiffs and the Class are entitled to actual, statutory, or nominal damages;

8. Whether restitution is appropriate; and

9. Whether injunctive relief is warranted to address ongoing harm.

145. **Typicality:** Plaintiffs' claims are typical of those of the Class because their PII was also compromised in the same breach, they suffered similar harms, and they seek the same relief as other Class Members.

146. **Adequacy of Representation:** Plaintiffs will fairly and adequately represent the Class. Their interests are aligned with those of the Class, and they are represented by competent counsel with experience in complex class actions and data breach litigation.

147. Plaintiff's Counsel are competent and experienced in litigation, and counsel is committed to vigorously protecting the interests of the Class and will adequately do so.

148. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on PowerSchool's systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

149. **Superiority**: A class action is the most efficient and appropriate method for resolving this controversy. Individual litigation would be impractical due to the relatively small damages per Class Member and would risk inconsistent outcomes and unnecessary burden on the courts. Class treatment allows for centralized adjudication and efficient case management.

COUNT I – NEGLIGENCE
(On behalf of Plaintiffs and the Class against Defendant)

150. PowerSchool owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

151. PowerSchool knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class members' PII and the importance of maintaining secure systems.

152. PowerSchool knew, or should have known, of the vast uptick in data breaches in recent years. PowerSchool had a duty to protect the PII of Plaintiffs and Class Members.

153. Given the nature of PowerSchool 's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, PowerSchool should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which PowerSchool had a duty to prevent.

154. PowerSchool breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiffs' and Class members' PII.

155. It was reasonably foreseeable to PowerSchool that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs 's and Class members' PII to unauthorized individuals.

156. But for PowerSchool's negligent conduct/breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

157. As a result of PowerSchool 's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II – NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Class against Defendant)

158. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

159. PowerSchool's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as PowerSchool, of failing to employ reasonable measures to protect and secure PII.

160. PowerSchool violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII and not complying with applicable industry standards. PowerSchool's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

161. PowerSchool's violations of Section 5 of the FTCA constitutes negligence *per se*.

162. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

163. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

164. It was reasonably foreseeable to PowerSchool that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII

by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

165. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of PowerSchool's violations of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III – BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Class against Defendant

166. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

167. Plaintiff and Class members either directly or indirectly gave PowerSchool their PII in confidence, believing that PowerSchool would protect that information. Plaintiff and Class members would not have provided PowerSchool with this information had they known it would not be adequately protected. PowerSchool's acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between PowerSchool and Plaintiff and Class Members. Due to this relationship, PowerSchool was required to act primarily for the benefit of its customers and students, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

168. PowerSchool has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the PII of Plaintiff and Class Members it collected.

169. As a direct and proximate result of PowerSchool's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury,

including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in PowerSchool's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV – BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class against Defendant)

170. Plaintiffs incorporate by reference all preceding allegations as though fully set forth herein.

171. Defendant promoted its educational technology services to schools, encouraging their use. As a result, Plaintiffs and Class Members used Defendant's products in connection with their educational activities and accepted the benefit of those services.

172. To access these services, Plaintiffs and Class Members had to provide their personally identifiable information (PII) to the Defendant. They disclosed this

information specifically to receive the educational services supported by the Defendant.

173. As described above, Plaintiffs and Class Members entrusted their PII to Defendant based, in part, on Defendant's repeated assurances that it would protect and secure user data. By providing their PII, Plaintiffs and Class Members entered into implied contracts with Defendant. Under those implied agreements, Defendant had an obligation to implement reasonable safeguards for Plaintiffs' and Class Members' PII and to provide timely and adequate notice of any data breaches, unauthorized disclosures, or known security vulnerabilities.

174. The educational services sought and received by Plaintiffs and Class Members were provided pursuant to mutually understood implied agreements. Those agreements required Defendant to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII and to notify them promptly in the event of any security incident involving that information.

175. Plaintiffs and Class Members would not have provided their PII to Defendant had it not represented that it would secure their data.

176. Nor would Plaintiffs and Class Members have disclosed their PII in the absence of the implied agreements described above.

177. Plaintiffs and Class Members satisfied their obligations under the implied contracts.

178. Defendant breached these implied contracts by failing to implement reasonable security measures to protect Plaintiffs' and Class Members' PII. Defendant also breached the contracts by failing to provide timely and adequate notice of the Data Breach, which resulted in unauthorized access to and disclosure of Plaintiffs' and Class Members' PII.

179. As a direct and proximate result of Defendant's breach, Plaintiffs and Class Members suffered and continue to suffer harm, including actual damages and losses as described herein.

COUNT V – UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class against Defendant)

180. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

181. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d)(2).

182. Plaintiff and Class Members conferred a monetary benefit upon PowerSchool in the form of monies paid for educational services or other services.

183. PowerSchool accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. PowerSchool also benefitted from the receipt of Plaintiff's and Class Members' PII.

184. As a result of PowerSchool's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

185. PowerSchool should not be permitted to retain the money belonging to Plaintiff and Class Members because PowerSchool failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

186. PowerSchool should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it because of the conduct and alleged Data Breach described above.

COUNT VI – VIOLATIONS OF THE MICHIGAN CONSUMER PROTECTION ACT, MICH. COMP. LAWS § 445.901, *et seq.* (On behalf of Plaintiffs and the Class against Defendant)

187. Plaintiffs incorporate by reference all preceding allegations as if fully set forth herein.

188. The Michigan Consumer Protection Act was created to protect Michigan consumers from unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce.

189. Plaintiff and Class members provided PII to Defendant pursuant to transactions (i.e., providing education) they engaged in with Defendant as customers and students.

190. Defendant has its principal place of business and headquarters in Michigan and transacts with Michigan consumers and students.

191. PowerSchool engaged in deceptive trade practices in the conduct of its business, in violation of Mich. Comp. Laws Ann § 445.901, including:

1. Representing that goods or services have characteristics that they do not have;

2. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

3. Advertising goods or services with intent not to provide them as advertised; and

4. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

192. PowerSchool's deceptive trade practices include:

1. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' PII, which was a direct and proximate cause of the Data Breach;

2. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

3. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class

Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

4. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' PII, including by implementing and maintaining reasonable security measures;

5. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and COPPA, 15 U.S.C. §§ 6501-6505;

6. Failing to timely and adequately notify Plaintiff, and class members of the Data Breach;

7. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class Members' PII; and

8. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and COPPA, 15 U.S.C. §§ 6501-6505.

193. PowerSchool's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of PowerSchool's data security and ability to protect the confidentiality of consumers' PII.

194. PowerSchool's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Class members, that their PII was not exposed and misled Plaintiff and the Class members into believing they did not need to take actions to secure their identities.

195. PowerSchool intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

196. Had PowerSchool disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, PowerSchool would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, PowerSchool was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff. PowerSchool accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because PowerSchool held itself out as maintaining a secure platform for PII data, Plaintiff and the Class members acted reasonably in relying on PowerSchool's misrepresentations and omissions, the truth of which they could not have discovered.

197. As a direct and proximate result of PowerSchool's deceptive trade practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

198. Class members are likely to be damaged by PowerSchool's ongoing deceptive trade practices.

199. Plaintiff and the Class members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

200. Accordingly, pursuant to Mich. Comp. Law Ann. § 445.901, et seq., Michigan Plaintiffs and Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Those damages are: (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; (c) present and increased risk arising from the identity theft and fraud.; and other miscellaneous incidental and consequential damages. In addition, given the nature of PowerSchool's conduct, Michigan Plaintiffs and Class members are entitled to all available statutory, exemplary, treble, and/or punitive damages and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from PowerSchool's unlawful conduct.

COUNT VII – VIOLATIONS OF THE MICHIGAN IDENTITY THEFT PROTECTION ACT Mich. Comp. Laws § 445.72 (On behalf of Plaintiffs and the Class against Defendant)

201. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

202. Defendant is a business that owns or licenses computerized data containing personal information as defined by Mich. Comp. Laws § 445.72(1)(h).

203. Defendant is subject to Mich. Comp. Laws § 445.72(2) and (3) because Defendant maintains computerized data that includes Plaintiffs' and Class Members' personal information, which Defendant does not own.

204. Plaintiffs' and Class Members' personal information includes data protected and covered under Mich. Comp. Laws § 445.72(1).

205. Defendant engaged in deceptive, unfair, and unlawful trade acts and practices by failing to reasonably safeguard Plaintiffs' and Class Members' PII, failing to prevent the Data Breach, and failing to mitigate the effects of the Data Breach.

206. Pursuant to this statute, Defendant is required to give immediate notice of a breach of a data system to the owners of PII. Defendant does not own the data that was subject to the Data Breach. Thus, Defendant was required to give immediate notice of the Data Breach to Plaintiffs and Class Members within thirty (30) days of discovery of the Data Breach.

207. Pursuant to this statute, Defendant is required to sufficiently notify Plaintiffs and Class Members if it discovers a security breach or receives notice of a security breach which may compromise PII in the most expedient time possible without unreasonable delay.

208. Defendant failed to timely or sufficiently disclose the Data Breach, a security breach, in violation of Mich. Comp. Laws § 445.72.

209. As a direct and proximate result of Defendant's violations Mich. Comp. Laws § 445.72, Plaintiffs and Class Members suffered damages, including: (i) theft of their PII, which includes highly sensitive medical information; (ii) imminent injury from identity theft; (iii) inability to mitigate the risks of identity theft and fraud due to Defendant's untimely disclosures of the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or mitigate the effects of the Data Breach, including, but not limited to, payment for credit monitoring services.

210. Plaintiffs and Class Members seek relief under Mich. Comp. Laws § 445.72(5), including actual damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, pray for relief and judgment against Defendant as follows:

A. An order declaring this action to be a proper class action, appointing Plaintiffs as Class Representatives and their counsel undersigned as Class Counsel, and requiring Defendant to bear the costs of class notice;

B. An order enjoining Defendant from engaging in the negligent, deceptive, unfair, and unlawful practices alleged in this Complaint;

C. An order requiring Defendant to develop, implement, and maintain reasonable security and privacy measures to protect Class Members' PII in accordance with applicable federal and state laws and industry standards;

D. An order requiring Defendant to engage in regular security audits and remedial measures to address any vulnerabilities identified in its systems;

E. An order requiring Defendant to provide extended credit monitoring and identity theft protection services to Plaintiffs and Class Members at Defendant's expense;

F. An order requiring Defendant to fund a data breach notification and

education program, including outreach to Class Members on how to mitigate harms from the Data Breach;

G. An order requiring Defendant to engage in a corrective or remedial advertising campaign to inform users and consumers of the nature of the Data Breach and the remedial steps being taken;

H. An order awarding declaratory relief, and any further retrospective or prospective injunctive relief permitted by law or equity, including enjoining Defendant from continuing the wrongful conduct alleged herein;

I. An order awarding restitution to restore all funds acquired by means of any act or practice declared by this Court to be unlawful, unfair, deceptive, or in violation of law, plus pre- and post-judgment interest;

J. An order requiring Defendant to disgorge all monies, revenues, and profits obtained by means of any wrongful or unlawful act or practice;

K. An order awarding Plaintiffs and the Class compensatory damages in an amount exceeding $5,000,000, to be determined at trial, for Defendant's negligence, negligence per se, breach of fiduciary duty, and breach of implied contract;

L. An order awarding Plaintiffs and the Class appropriate actual and statutory damages, including under the Michigan Consumer

Protection Act and Michigan Identity Theft Protection Act;

M. An order awarding Plaintiffs and the Class restitutionary damages for unjust enrichment;

N. An order awarding Plaintiffs and the Class punitive and/or exemplary damages to deter future misconduct;

O. An order awarding Plaintiffs and the Class the costs of prosecuting this action, including expert witness fees;

P. An order awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law;

Q. An order awarding Plaintiffs and the Class pre-judgment and post-judgment interest; and

R. Granting any other relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: April 1, 2025

Respectfully submitted,

BROOKS KUSHMAN P.C.

/s/ John P. Rondini
John P. Rondini (P72254)
Matthew M. Jakubowski (P63194)
Muhammad A. Siwani (P87435)

150 W. Second St., Suite 400N
Royal Oak, MI 48067-3846
(248) 358-4400 / Fax: (248) 358-3351
Email: jrondini@brookskushman.com
mjakubowski@brookskushman.
msiwani@brookskushman.com

Attorneys for Plaintiffs